**PROTECTED A**

# SUMMARY OF NOTABLE SUBMISSIONS ON LAWFUL ACCESS

## *Overview*

Public Safety (PS) received 35 notable submissions which addressed the *Green Paper* theme of "Investigative Capabilities in a Digital World" (hereafter, "lawful access"). Stakeholders from the law enforcement, civil society, academic, and communications service provider (CSP) sectors, as well as Federal, Provincial and Territorial (FPT) Privacy Commissioners addressed this issue. In addition to the four policy areas discussed in the *Green Paper*, stakeholders addressed issues such as accountability for lawful access powers, governance and safeguards for metadata-related activities, the reform of existing surveillance law, bulk collection powers, and the extraterritorial application of judicial orders.

## *Skepticism of the Need for New Investigatory Powers*

Across all themes, stakeholders believed it was unclear why existing statutory powers were inadequate for the needs of investigators. Many stakeholders called on the Government to provide clear evidence to justify that changes are necessary.

It was not clear to several civil society, academic, and CSP stakeholders that the requirement to seek a judicial order to obtain basic subscriber information (BSI) would unduly impede investigations. Some of these stakeholders believed the Government should take steps to improve the efficiency of the court system rather than introduce new laws.

Many civil society, academic, and CSP stakeholders, as well as FPT Privacy Commissioners questioned the necessity of creating universal data retention requirements given that data preservation powers were enacted in 2015.

FPT Privacy Commissioners and academic stakeholders also questioned the need for encryption-specific legislation, reasoning that investigators could use assistance order powers to address encryption-related challenges.

## *Perceived Need to Reform Existing Investigatory Powers*

Many civil society stakeholders recommended reforming existing legislation governing surveillance activities, rather than introducing new powers. These included stakeholders believed the law has not kept with developments in technology nor evolved in response to disclosures of certain investigative activities.

Specific proposals included:

- Harmonize the authorization standards for warranted powers exercised by different agencies – **Profs. Craig Forcese and Kent Roach (Academics)**
- Legal protections for solicitor-client privileged information that might be collected under judicially-authorized powers – **(Civil Society)**
- Designate CSPs involved in surveillance as state actors that must comply with the *Charter* – **(Civil Society)**
- Subject any search of electronic devices to the highest standards of privacy protection available under the *Charter* – **(Civil Society)**
- Use the International Principles on the Application of Human Rights to Communications Surveillance (which were developed by civil society organization, human rights and privacy advocates, and criminal lawyers in 2013) to guide reforms to "mass" surveillance – **(Academics)**

## ***Accountability***

In their discussion of lawful access issues, civil society stakeholders, in particular, believed it is necessary for the Government to enhance accountability mechanisms. Specific proposals included:

- Accompany any lawful access measures with proportional accountability measures – **(Civil Society),**
- All Government bodies and the private sector should increase public reporting on lawful access activities – **FPT Privacy Commissioners**
- Existing accountability bodies should be given powers to enforce compliance –
- Existing accountability bodies should receive more resources –
- Canadian should be entitled to access a summary description of Government-held information "associated with their name," subject to reasonable limits –

# CONSULTATION ON NATIONAL SECURITY
## SUBMISSION SUMMARY: DIGITAL WORLD

**PROTECTED A**

## *Private Sector Compliance*

A prominent concern for CSP stakeholders was that new laws could adversely impact their business operations and competitiveness. This concern was most prominent with regard to the issues of intercept capable networks and data retention. In addition to CSPs, some civil society stakeholders noted the potential for new legislation to create additional costs for industry that would ultimately be passed to consumers. There were also concerns from some CSP stakeholders that new requirements would disproportionately impact smaller CSPs or those serving rural or remote areas. Stakeholders offered an array of recommendations, including:

- The Government should compensate CSPs for the costs of complying with new requirements – **(Civil Society)**
- The Government should compensate CSPs for damages incurred as a result of any breaches of data that would have been deleted if not for retention requirements –
- 
- Any new law should include a twenty-four month grace period for companies to integrate new requirements –
- Smaller CSPs should be exempt from having to "immediately " develop intercept capability requirements -
- Any new requirements should be mandatory for all CSPs to ensure market competitiveness –
- Any intercept capability requirement should reflect industry standards developed n the US or Europe –
- Further consultation is necessary on any specific intercept capability proposals –

In addition, some civil society and academic stakeholders expressed concerns over the potential for CSPs to use intercept capabilities or retained data for commercial activities. These stakeholders noted the importance of legal safeguards to ensure that new capabilities are only used pursuant to lawful investigators.

# CONSULTATION ON NATIONAL SECURITY
## SUBMISSION SUMMARY: DIGITAL WORLD

**PROTECTED A**

### *Intercept-Capable Networks*

While they did not express support for this proposal, most CSP stakeholders did not outright oppose the introduction of intercept capability requirements either. Rather, these CSPs stakeholders recommended that, should intercept capability requirements be introduced, this must be accompanied by measures to ensure that new obligations do not interfere with business operations or competitiveness (see the discussion on privacy sector compliance above). However, some civil society organizations (including [redacted]) opposed the introduction of any intercept capability requirements. Only law enforcement stakeholders expressed unqualified support for intercept capability.

### *Data Retention*

While law enforcement stakeholders supported introducing mandatory minimum data retention periods, many civil society and academic stakeholders opposed any such proposal. CSP and civil society stakeholders which did not express outright opposition to data retention still noted serious concerns regarding the potential impact of such measure on the privacy of Canadians and on the security of their data. Stakeholders recommended that any data retention regime be accompanied by new safeguards to protect privacy rights and mitigate security risks. There were also concerns regarding the costs generated by new obligations on CSPs (discussed above).

Notable ideas for data retention safeguards included:

- Introducing short mandatory retention periods – [redacted] **(Civil Society)**, [redacted] **(Academic)**
- Varying mandatory retention periods depending on the sensitivity of the data involved - [redacted] **(Civil Society)**
- Mandating security standards as part of any retention regime – [redacted]
- Requiring judicial authorization to access retained data – [redacted] **(Independent Expert)**
- Requiring judicial authorization to retain data beyond the minimum retention period – [redacted]

# CONSULTATION ON NATIONAL SECURITY
## SUBMISSION SUMMARY: DIGITAL WORLD

**PROTECTED A**

## *Lawful Access to BSI*

Most stakeholders – spanning the civil society, academic, and CSP sectors – believed that investigators should require judicial authorization in order to access BSI. Related to this, many academic and civil society sectors expressed the view that BSI is sensitive personal information, particularly in relation to IP addresses. However, two academic stakeholders who opposed administrative access to BSI still supported legislative amendments to allow police to obtain BSI without a court order in life-threatening situations.

Notable policy ideas regarding access to BSI included:

- Create a "graduated scale" for access to BSI, where procedural and evidentiary requirements for access depend on the likelihood a crime has been or will be committed, the severity of that crime, and the urgency for disclosure - **(Civil Society)**
- Establish clear legal prohibitions against the voluntary disclosure of BSI by CSPs. **(Academia)**
-

Some CSP and civil society stakeholders did not oppose the creation of a regime for administrative access to BSI, but believed that any such regime would require special safeguards to uphold privacy rights and protect against abuse. Notable ideas for safeguards included:

- Any access regime requires a clear governance system to prevent mass BSI requests or "fishing expeditions."
- Investigators should be prohibited from using BSI in any investigation other than the investigation for which it was originally obtained. **(Civil Society)**

s.13(1)(c)
s.19(1)
s.20(1)(c)
s.20(1)(d)



# CONSULTATION ON NATIONAL SECURITY
## SUBMISSION SUMMARY: DIGITAL WORLD

**PROTECTED A**

Among stakeholders who supported mandatory data retention, the recommended retention period ranged from 6 months ( , and ) to between 12 and 24 months (the , a civil society organization with strong ties to law enforcement).

## *Encryption*

Stakeholders across the civil society, academic, and CSP sectors supported strong encryption tools, believing them to be important for legitimate aims such as cybersecurity, privacy, and freedom of expression. Stakeholders broadly opposed "exceptional access" measures (such as key escrow or technical "backdoors") given the significant security and privacy risks associated with such measures. However, some CSP stakeholders believed that CSPs could be expected to decrypt data if those providers held the necessary keys to do so and were not expected to provide access to data encrypted by third parties.

Many civil society and academic stakeholders opposed any proposal to compel individuals to disclose their passwords, noting the constitutional risks this would involve.

FPT Privacy Commissioners and the Internet Society Canada Chapter believed the Government should explore technical solutions to address encryption challenges for investigators.

Notable policy ideas regarding encryption included:

- The Government should commission research into encryption solutions, in particular through the Centre for Applied Cryptographic Research at the University of Waterloo. **(Civil Society)**
- 
- Prohibit the Canada Border Services Agency from compelling password disclosure without a warrant –

# CONSULTATION ON NATIONAL SECURITY
## SUBMISSION SUMMARY: DIGITAL WORLD

**PROTECTED A**

## *Metadata*

Several stakeholders discussed metadata issues that were beyond the scope of the *Green Paper*. Stakeholders noted concerns over recent controversies involving metadata, including the use of IMSI catchers by Canadian police, the Federal Court decision regarding the Canadian Security Intelligence Service (CSIS) Operational Data Analysis Centre, and the metadata-related activities of the Communications Security Establishment (CSE). Notable policy proposals included:

- Conduct a focused public consultation on the use of IMSI catchers – [redacted]
- Consider German law as a model for the governance of IMSI catcher use – [redacted]
- Subjecting CSIS and law enforcement to the same authorization standards to collect metadata – [redacted] **(Academic)**
- Subject metadata collection to judicial authorization – **FPT Privacy Commissioners**
- Limit metadata collection to the investigation of serious crimes prescribed by law and only where other techniques have failed – **FPT Privacy Commissioners**
- Introduce legal standards for the retention and destruction of collected metadata – [redacted] **FPT Privacy Commissioners**
- Introduce new legal safeguards for the collection, use, and disclosure of metadata by CSE - **FPT Privacy Commissioners**

## *Other Issues*

Some academic and civil society organizations expressed opposition to any **bulk intelligence collection powers**. Recommendations on this issue included:

- Create a new warrant process for "mass surveillance technologies and techniques", possibly modeled on German laws governing IMSI catcher use – [redacted]
- Build more internet infrastructure and increase domestic CSP cooperation in order to protect Canadian traffic from perceived US surveillance - [redacted] **(Academic)**

Government of Canada / Gouvernement du Canada

Canada

# CONSULTATION ON NATIONAL SECURITY

## SUBMISSION SUMMARY: DIGITAL WORLD

**PROTECTED A**

Two civil society organizations made recommendations regarding the issue of **extraterritorial application of judicial orders:**

- Do not introduce legislation requiring a person in Canada to produce or provide information located overseas – **(Civil Society)**
- Improve the Mutual Legal Assistance Treaty Process – **(Civil Society)**